U.S. SECURITIES AND
EXCHANGE COMMISSION

REPORT NO. 574
NOVEMBER 15, 2022

OFFICE OF
INSPECTOR
GENERAL

OFFICE OF AUDITS

Fiscal Year 2022 Independent Evaluation of the SEC's Implementation of the Federal Information Security Modernization Act of 2014

This report contains non-public information about the U.S. Securities and Exchange Commission's information technology program. We redacted the non-public information to create this public version. All redactions are pursuant to Freedom of Information Act exemption (b)(7)(E) unless otherwise stated.

REDACTED FOR PUBLIC RELEASE

OFFICE OF
INSPECTOR GENERAL

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

MEMORANDUM

November 15, 2022

TO: Kenneth Johnson, Chief Operating Officer

FROM: Nicholas Padilla, Acting Inspector General

SUBJECT: *Fiscal Year 2022 Independent Evaluation of the SEC's Implementation of the Federal Information Security Modernization Act of 2014*, Report 574

Attached is the Independent Auditor's Report on the Fiscal Year 2022 Independent Evaluation of the U.S. Securities and Exchange Commission's (SEC or agency) Implementation of the Federal Information Security Modernization Act of 2014 (FISMA). We contracted with Kearney & Company, P.C. (referred to as "Kearney") to conduct this independent evaluation. The SEC's Office of Inspector General (OIG) monitored Kearney's work to ensure it met professional standards and contractual requirements. Kearney conducted the evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation.*

Kearney is wholly responsible for the attached evaluation report and the conclusions expressed therein. The OIG monitored Kearney's performance throughout the evaluation and reviewed Kearney's report and related documentation.

Kearney reported that the SEC made progress in improving its information security program by institutionalizing the use of advanced risk management technologies; developing a standard hardware taxonomy across the agency; and updating relevant components of the agency's interconnection inventory. However, the agency faced challenges, to include, but not limited to, documenting the results of privacy risk assessments, integrating formal lessons learned on the effectiveness of incident handling policies and procedures; and completing Business Impact Analyses for its information systems.

As described in the attached report, Kearney identified opportunities for improvement in key areas and made 13 new recommendations to strengthen these areas of the SEC's information security program. As a result, Kearney noted that the agency's information security program did not meet the FY 2022 Inspector General FISMA Reporting Metrics' definition of "effective".

On September 21, 2022, we provided management with a draft of Kearney's report for review and comment. In the agency's October 12, 2022 response, management concurred with Kearney's recommendations. Kearney included management's response as Appendix IV of this report.

To improve the SEC's information security program, we urge management to take action to address areas of potential risk identified in this report. Please provide the OIG with a written corrective action plan within the next 45 days that addresses the recommendations. The corrective action plan should include information such as the responsible official/point of contact, timeframe for completing the required actions, and milestones identifying how the SEC will address the recommendations.

We appreciate management's courtesies and cooperation during the evaluation. If you have question, please contact me or Rebecca L. Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects.

Attachment

cc: Gary Gensler, Chair
Prashant Yerramalli, Chief of Staff, Office of Chair Gensler
Heather Slavkin Corzo, Policy Director, Office of Chair Gensler
Ajay Sutaria, GC Counsel, Office of Chair Gensler
Kevin Burris, Counselor to the Chair and Director of Legislative and Intergovernmental Affairs
Scott Schneider, Counselor to the Chair and Director of Public Affairs
Philipp Havenstein, Operations Counsel, Office of Chair Gensler
Hester M. Peirce, Commissioner
Benjamin Vetter, Counsel, Office of Commissioner Peirce
Caroline A. Crenshaw, Commissioner
Malgorzata Spangenberg, Counsel, Office of Commissioner Crenshaw
Mark T. Uyeda, Commissioner
Holly Hunter-Ceci, Counsel, Office of Commissioner Uyeda
Jaime Lizárraga, Commissioner
Laura D'Allaird, Counsel, Office of Commissioner Lizárraga
Parisa Haghshenas, Counsel, Office of Commissioner Lizárraga
Dan Berkovitz, General Counsel
Shelly Luisi, Chief Risk Officer
Jim Lloyd, Audit Coordinator/Assistant Chief Risk Officer, Office of Chief Risk Officer
David Bottom, Director/Chief Information Officer, Office of Information Technology
James Scobey, Chief Information Security Officer, Office of Information Technology
Bridget Hilal, Branch Chief, Cyber Risk and Governance Branch, Office of Information Technology

Fiscal Year 2022 Independent Evaluation of the U.S. Securities and Exchange Commission's Implementation of the Federal Information Security Modernization Act of 2014

November 15, 2022

KEARNEY& COMPANY

Point of Contact Phil Moore,
1701 Duke Street, Suite 500
Alexandria, VA 22314
703-931-5600, 703-931-3655 (fax)
Phil.Moore@kearneyco.com
Kearney & Company, P.C.'s TIN is 54-1603527, DUNS is 18-657-6310, Cage Code is 1SJ14

Cover Letter

November 15, 2022

Mr. Nicholas Padilla
Acting Inspector General
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549

Dear Mr. Padilla:

This report presents the results of Kearney & Company, P.C's (referred to as "Kearney," "we," and "our" in this report) independent evaluation of the U.S. Securities and Exchange Commission's (referred to as "SEC" or "agency") information security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires all Federal agencies to develop, document, and implement an agency-wide information security program to protect its information and information systems, including those provided or managed by another agency, contractor, or other source. Additionally, FISMA requires each Federal agency Inspector General (IG) or a contracted independent external auditor to conduct an annual independent evaluation to determine the effectiveness of its information security program and practices. Kearney conducted this independent evaluation of the SEC's information security program and practices in support of the SEC Office of Inspector General (OIG) in accordance with the Council of Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Kearney's evaluation included inquiries, observations, and inspection of SEC documents and records, as well as direct testing of controls. We are pleased to provide our report, entitled *Fiscal Year (FY) 2022 Independent Evaluation of the U.S. Securities and Exchange Commission's Implementation of the Federal Information Security Modernization Act of 2014.*

The objectives of this evaluation were to assess the effectiveness of the SEC's information security program and practices and respond to the *FY 2022 IG FISMA Reporting Metrics*. Kearney's methodology for the FY 2022 FISMA evaluation included testing the effectiveness of selected security controls the SEC has implemented in eight sampled information systems for compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated September 2020. The *FY 2022 IG FISMA Reporting Metrics* utilize a maturity model and request that IGs evaluate and rate the effectiveness of security controls for each of the five *NIST Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) function areas (i.e., Identify, Protect, Detect, Respond, and Recover). Additionally, the *FY 2022 IG FISMA Reporting Metrics* were updated to introduce the concept of "core metrics." In FY 2022, instead of testing all 57 metrics across the nine FISMA domains included in the *FY 2021 IG FISMA Reporting Metrics*, 20 core metrics were selected from the FY 2021 metrics. The *FY 2022 IG FISMA Reporting Metrics* states that the FY 2022 core metrics were chosen based on alignment with Executive Order 14028, *Improving the Nation's Cybersecurity*, as well as recent Office of Management and Budget guidance to agencies in furtherance of the modernization of Federal cybersecurity. Finally, to achieve an effective level of information security under the maturity model, agencies must reach Level 4: *Managed and Measurable.*

Since FY 2021, the SEC's Office of Information Technology (OIT) improved aspects of its information security program. Among other actions taken, OIT made progress in institutionalizing the use of advanced risk management technologies, developing a standard hardware taxonomy across the agency, and updating relevant components of the agency's interconnection inventory. Although the SEC has strengthened its program since the last FISMA evaluation, Kearney noted that the agency's information security program did not meet Level 4: *Managed and Measurable* and, therefore, was not effective. As shown in **TABLE 1** below, there was a significant decrease in both the overall Security Training domain rating (from *Optimized* in FY 2021 to *Defined* in FY 2022) and the Contingency Planning domain rating (from *Managed and Measurable* in FY 2021 to *Consistently Implemented* in FY 2022). We determined that these decreases were primarily due to changes in the methodology for the FY 2022 assessment. Specifically, the FY 2022 assessment included fewer metrics overall than the FY 2021 evaluation.

TABLE 1. Summary of SEC FISMA Ratings

Domain	Assessed Rating By Fiscal Year (FY)	
	2022	2021
Risk Management	Level 3: *Consistently Implemented*	Level 3: *Consistently Implemented*
Supply Chain Risk Management	Level 1: *Ad Hoc*	Level 1: *Ad Hoc*
Configuration Management	Level 2: *Defined*	Level 2: *Defined*
Identity and Access Management	Level 2: *Defined*	Level 2: *Defined*
Data Protection and Privacy	Level 3: *Consistently Implemented*	Level 3: *Consistently Implemented*
Security Training	Level 2: *Defined*	Level 5: *Optimized*
Information Security Continuous Monitoring	Level 3: *Consistently Implemented*	Level 3: *Consistently Implemented*
Incident Response	Level 4: *Managed and Measurable*	Level 4: *Managed and Measurable*
Contingency Planning	Level 3: *Consistently Implemented*	Level 4: *Managed and Measurable*

Source: Kearney-generated based on FYs 2021 and 2022 CyberScope metric responses

Our report includes 13 new recommendations to strengthen the SEC's information security program. As our report highlights, while the SEC made improvements in many aspects of its information security program, opportunities exist for the SEC to improve its performance in all nine *FY 2022 IG FISMA Reporting Metrics* domains. Opportunities for improvement remain in key areas such as: 1) maintaining a comprehensive and accurate [redacted]; 2) documenting the results of privacy risk assessments; 3) maintaining a complete [redacted]; 4) defining policies and procedures for cybersecurity and supply chain risk management requirements for external providers; 5) deploying and maintaining [redacted]; 6) implementing policies, procedures, and processes for [redacted]; 7) completing [redacted] for information systems; 8) managing and measuring the effectiveness of [redacted]; 9) [redacted]; 10) implementing [redacted] for information systems; 11) transitioning to [redacted]; 12) integrating formal lessons learned on the effectiveness of incident handling policies and procedures; and 13) completing Business Impact Analyses for its information systems. Acting on these opportunities for improvement will help minimize the risk of unauthorized disclosure, modification, use, and disruption of the SEC's sensitive, non-public information, as well as assist the SEC's information security program reach the next maturity level.

In closing, we appreciate the courtesies extended to the Kearney Evaluation Team by the SEC during this engagement.

Sincerely,

Kearney & Company

Kearney & Company, P.C.

November 15, 2022

Contents

Page #

Tables

Page #

Figure

Page #

Abbreviations

BIA	Business Impact Analysis
CDM	Continuous Diagnostic and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISA	Cybersecurity & Infrastructure Security Agency
Cybersecurity Framework	National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure of Cybersecurity*
DBaaS	Dashboard as a Service
DHS	Department of Homeland Security
DNS	Domain Name System
[redacted]	[redacted]
[redacted]	[redacted]
eGRC	Enterprise Risk, Governance, and Compliance
ENF	Division of Enforcement
FIPS	Federal Information Processing Standards
FISMA	Federal Information Systems Modernization Act of 2014
FOIA	Freedom of Information Act
FY	Fiscal Year
GAO	U.S. Government Accountability Office
GSS	General Support System
HVA	High Value Asset
ICT	Information and Communications Technology
IG	Inspector General
ISCM	Information Security Continuous Monitoring
IT	Information Technology
[redacted]	[redacted]
Kearney	Kearney & Company, P.C.
[redacted]	[redacted]

REDACTED FOR PUBLIC RELEASE

MOU	Memorandum of Understanding
[redacted]	[redacted]
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PISA	Privacy Information Security Awareness
PL	Public Law
PUB	Publication
Rev.	Revision
[redacted]	[redacted]
SaaS	Software as a Service
SCRM	Supply Chain Risk Management
SEC or agency	U.S. Securities and Exchange Commission
SP	Special Publication
SSP	System Security Plan
[redacted]	[redacted]
[redacted]	[redacted]

Background and Objectives

Background

On December 18, 2014, the President signed into law the Federal Information Security Modernization Act of 2014 (FISMA) (Public Law [PL] 113-283). FISMA provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets and a mechanism for oversight of Federal information security programs. FISMA also requires agencies to develop, document, and implement an agency-wide information security program to provide information security for the data and information systems that support the operations and assets of the agency.

In addition, FISMA requires each Federal agency Inspector General (IG) or a contracted independent external auditor to conduct an annual independent evaluation to determine the effectiveness of its information security program and practices. This assessment includes testing and assessing the effectiveness of information security policies, procedures, and practices, as well as a subset of information systems. In support of these requirements, the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) issued guidance to IGs on FISMA reporting for fiscal year (FY) 2022.

In accordance with FISMA, the U.S. Securities and Exchange Commission (SEC or agency) aims to implement an effective and exemplary information security program across the agency. The *FY 2022 IG FISMA Reporting Metrics* establish that an effective agency has reached or exceeded Level 4: *Managed and Measurable* in a simple majority of the nine IG FISMA Reporting Metrics Assessment Domains mapped to the five cybersecurity function areas, shown in **TABLE 2**.

TABLE 2. Cybersecurity Function Areas Mapped to *FY 2022 IG FISMA Reporting Metrics* Assessment Domains

Cybersecurity Function Areas	*FY 2022 IG FISMA Reporting Metrics* Assessment Domains
Identify	Risk Management
	Supply Chain Risk Management (SCRM)
Protect	Configuration Management
	Identity and Access Management
	Data Protection and Privacy
	Security Training
Detect	Information Security Continuous Monitoring (ISCM)
Respond	Incident Response
Recover	Contingency Planning

Source: Kearney & Company, P.C. (Kearney)-generated from FY 2022 IG FISMA Reporting Metrics

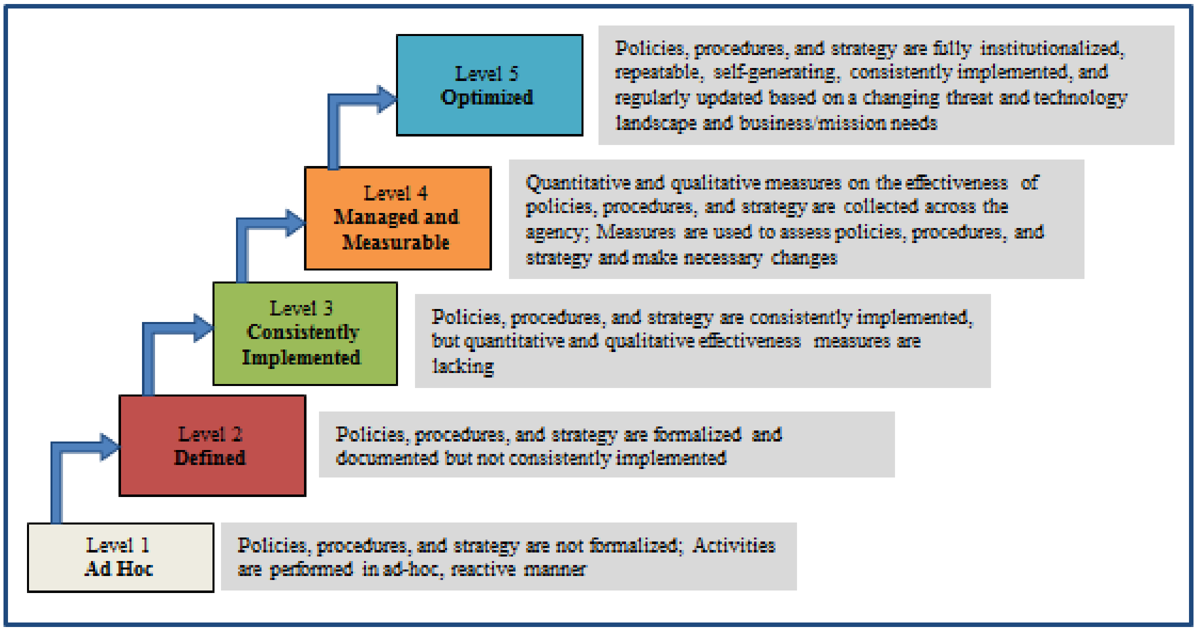
Change in Metrics and Assessment Methodology: In FY 2022, the *FY 2022 IG FISMA Reporting Metrics* were updated to introduce the concept of "core metrics" and to include consideration for National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 5. The core metrics utilized in FY 2022 were 20 metrics that "should provide sufficient data to determine the effectiveness of an agency's information security program with a high level of confidence."[1] Instead of

[1] *FY 2022 IG FISMA Reporting Metrics*

testing all 57 metrics across the nine FISMA domains included in the *FY 2021 IG FISMA Reporting Metrics*, in FY 2022, we tested only the 20 core metrics. Lastly, in FY 2022, CIGIE published an updated *FY 2022 Core IG FISMA Metrics Evaluation Guide* that includes suggested artifacts, types of evidence, and analysis that IGs can perform to determine maturity.

As shown in **FIGURE 1**, the foundation levels (Levels 1 and 2) of the maturity model ensure that agencies develop sound policies and procedures, whereas the advanced levels capture the extent to which agencies institutionalize those policies and procedures (Level 3), establish performance measures (Level 4), and aim to improve and optimize performance against established goals (Level 5).

FIGURE 1. IG Assessment Maturity Levels


Level 5
Optimized
Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs
Level 4
Managed and Measurable
Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the agency; Measures are used to assess policies, procedures, and strategy and make necessary changes
Level 3
Consistently Implemented
Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking
Level 2
Defined
Policies, procedures, and strategy are formalized and documented but not consistently implemented
Level 1
Ad Hoc
Policies, procedures, and strategy are not formalized; Activities are performed in ad-hoc, reactive manner

Source: Kearney-generated based on the FY 2021 IG FISMA Reporting Metrics

The maturity model also summarizes the status of agencies' information security programs, encourages transparency on what has been accomplished and what still needs to be implemented to improve the information security program, and helps ensure consistency across the IGs in annual FISMA reviews. Within the context of the maturity model, Level 4: *Managed and Measurable* represents an effective level of security.

Responsible Office: The SEC's Office of Information Technology (OIT) holds overall management responsibility for the SEC's information technology (IT) program, including information security. OIT establishes IT security policies and provides technical support, assistance, direction, and guidance to the SEC's divisions and offices. The Chief Information Officer directs OIT and is responsible for ensuring compliance with applicable information security requirements. The Chief Information Security Officer is responsible, in part, for developing, maintaining, centralizing, and monitoring ongoing adherence to the SEC's *Information Security Program Plan* and supporting the Chief Information Officer in annually reporting on the effectiveness of the SEC's information security program.

Prior Audits and Evaluations: As of May 25, 2022, the SEC took corrective action sufficient to close 12 recommendations from prior-year FISMA reports. Specifically, within FY 2022, the SEC took actions to close two of four open recommendations from the OIG's audit of the SEC's compliance with FISMA for FY 2017[1] (FY 2017 FISMA audit), dated March 30, 2018; two of three open recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2018[2] (FY 2018 FISMA evaluation), dated December 12, 2018; four of four open recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2019[3] (FY 2019 FISMA evaluation), dated December 18, 2019; three of five open recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2020[4] (FY 2020 FISMA evaluation), dated December 21, 2020; and one of seven open recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2021[5] (FY 2021 FISMA evaluation), dated December 21, 2021. In total, as of May 25, 2022, the SEC has remediated 18 of the 20 recommendations from the FY 2017 FISMA audit, 10 of the 11 recommendations from the FY 2018 FISMA evaluation, nine of the nine recommendations from the FY 2019 FISMA evaluation, five of seven recommendations from the FY 2020 FISMA evaluation, and one of eight recommendations from the FY 2021 FISMA evaluation.

[1] U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017*, Report No. 546; March 30, 2018 (hereafter referred to as "FY 2017 FISMA audit")

[2] U.S. Securities and Exchange Commission, Office of Inspector General, *Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security*, Report No. 552; December 12, 2018 (hereafter referred to as "FY 2018 FISMA evaluation")

[3] U.S. Securities and Exchange Commission, Office of Inspector General, *Fiscal Year 2019 Independent Evaluation of SEC's Implementation of the Federal Information Security*, Report No. 558; December 18, 2019 (hereafter referred to as "FY 2019 FISMA evaluation")

[4] U.S. Securities and Exchange Commission, Office of Inspector General, *Fiscal Year 2020 Independent Evaluation of SEC's Implementation of the Federal Information Security*, Report No. 563; December 21, 2020 (hereafter referred to as "FY 2020 FISMA evaluation")

[5] U.S. Securities and Exchange Commission, Office of Inspector General, *Fiscal Year 2021 Independent Evaluation of SEC's Implementation of the Federal Information Security*, Report No. 570; December 21, 2021 (hereafter referred to as "FY 2021 FISMA evaluation")

Results

Domain #1: Risk Management

The NIST Cybersecurity Framework considers risk management as the ongoing process of identifying, assessing, and responding to risk. Risk management practices include establishing the context for risk-related activities, assessing risk, responding to risk once determined, and monitoring risk over time. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, dated March 2011, states that in order to integrate the risk management process throughout the organization, a three-tiered approach is employed that addresses risk at the following levels: organizational (Tier 1), mission/business processes (Tier 2), and information systems (Tier 3).

Kearney assessed the SEC's risk management program and determined that the program's assessed maturity level is Level 3: *Consistently Implemented*, meaning the SEC consistently implemented its continuous monitoring policies, procedures, and strategies for its risk management processes, but quantitative and qualitative effectiveness measures were lacking. While the agency's assessed maturity remained at Level 3: *Consistently Implemented* between FYs 2021 and 2022, it has not fully implemented the recommendations identified in prior years; therefore, certain previously identified conditions still exist.

Prior-Year Findings: Specifically, in the FY 2021 FISMA evaluation, Kearney determined that the SEC did not develop, document, or implement a process:

- For consistently implementing [redacted] within the agency's [redacted]
- To clearly define requirements for consistently completing and maintaining Federal Information Processing Standards (FIPS) Publication (PUB) 199 categorization worksheets for all system types.

Similarly, Kearney determined that many of the weaknesses within the SEC's risk management program identified during the FY 2021 FISMA evaluation remained present in FY 2022, as listed below:

- While the SEC has developed an approved software list and software license inventory within its [redacted], the agency has not completely [redacted]. Specifically, [redacted]
- While the SEC developed FIPS PUB 199 categorization worksheets for the sampled systems, one of the eight (12.5 percent) sampled systems [redacted] did not have a categorization worksheet or consider NIST SP 800-60, Volume 1, Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, dated August 2008, as required by the agency's *Security Assessment and Authorization Operating Procedures*. Finally, Kearney noted that, after the scope period of the evaluation, OIT

took steps to update its [redacted] FIPS PUB 199 categorization worksheet to include consideration for NIST SP 800-60.

These control weaknesses occurred for a variety of reasons. Due to a technical limitation in the agency's asset management system, OIT was unable to [redacted]. Further, OIT was still working to mature its Mobile Device Management solution. Finally, the FIPS PUB 199 categorization worksheet for one system was outdated; however, as part of its 2022 security assessment, OIT has worked to review and update the outdated [redacted] FIPS PUB 199 worksheet. Kearney is not making any new recommendations in relation to the prior-year findings noted above, as the SEC is working to address the prior-year FISMA recommendations. See **Appendix II: Open FISMA Recommendations**.

Current-Year Findings: Kearney has identified additional opportunities for the agency to mature its risk management program. See the findings detailed below:

In addition to the prior-year findings, Kearney identified new weaknesses related to the agency's system [redacted], privacy risk assessments, and [redacted].

The SEC did not consistently maintain a comprehensive and accurate [redacted]. The *FY 2022 IG FISMA Reporting Metrics* measure the extent to which agencies consistently maintain comprehensive and accurate inventories of system interconnections. The NIST Cybersecurity Framework, Control ID.AM-1, requires that systems within the organization are inventoried, and Control ID.AM-4, requires that external information systems are catalogued. Further, the SEC's *Memorandum of Understanding/Agreement (MOU/A) Interconnection Security Agreement, and Interagency Agreement Policy* states that OIT Security must keep an inventory of all agreements that have been provided in the OIT enterprise Risk, Governance, and Compliance (eGRC) system. Finally, the *MOU/A Policy* states that the eGRC system is required to track the name of the system, agreement type, and expiration date, as well as store a copy of the document as an attachment.

The SEC defined the policies, procedures, and processes for its inventory of system interconnections and updated the relevant components of the inventory; however, [redacted] and [redacted].

This occurred, in part, because OIT did not consistently implement its process to review its SSPs for [redacted]. Further, the agency did not take steps to ensure that [redacted]. Finally, in the time since fieldwork was completed, OIT updated its eGRC system to include the missing system interconnections in the [redacted] SSP.

Without the consistent maintenance of a comprehensive and accurate [redacted]. In addition, without tracking [redacted], the SEC risks breaking terms or conditions defined within [redacted].

The SEC did not always document the results of its privacy risk assessments within the agency's [redacted]. The *FY 2022 IG FISMA Reporting Metrics* measure the extent to which agencies utilize the results of privacy risk assessments and document the results of these assessments within their cybersecurity risk registers. Further, the reporting metrics measure the extent to which agencies utilized the results of their system-level risk assessments, along with other inputs, to perform and maintain agency-wide cybersecurity and privacy risk assessments. Additionally, NIST Interagency Report 8286 states: "cybersecurity risk inputs to ERM programs should be documented and tracked in written cybersecurity risk registers that comply with the ERM program guidance."

The SEC consistently integrated its risk management processes with its privacy analyses through the use of [redacted]. In addition, the SEC consistently integrated privacy requirements into its risk management process by documenting the results of its privacy risk assessments [redacted]; however, the agency did not always document the results of its privacy risk assessments within its [redacted].

This occurred, in part, because the agency did not develop a process for documenting the results of its privacy risk assessments within its cybersecurity risk register for all of its information systems.

Without documenting the results of privacy risk assessments into the agency's [redacted] for all of its information systems, the SEC may not be able to adequately quantify or aggregate security risks, normalize cybersecurity risk information across organizational units, or prioritize operational risk response.

The SEC did not consistently [redacted]. The *FY 2022 IG FISMA Reporting Metrics* measure the extent to which agencies utilize standard data elements/taxonomy to consistently maintain up-to-date inventories of hardware assets connected to their networks. Additionally, NIST SP 800-53, Rev. 5, CM-7 (9), states: "hardware components provide the foundation for organizational systems and the platform for the execution of authorized software programs. Managing the inventory of hardware components and controlling which hardware components are permitted to be installed or connected to organizational systems is essential in order to provide adequate security."

The SEC defined its policies and procedures for developing a complete and accurate inventory of hardware assets. However, the agency did not [redacted].

This occurred, in part, because the SEC did not [redacted].

Without the [redacted].

Recommendations, Management's Response, and Evaluation of Management's Response

To mature the U.S. Securities and Exchange Commission's risk management program, Kearney & Company, P.C. recommends that the Office of Information Technology continue to work to close open prior-year recommendations. See **Appendix II: Open FISMA Recommendations**.

Additionally, Kearney & Company, P.C. recommends that the U.S. Securities and Exchange Commission's Office of Information Technology:

Recommendation 1: Consistently implement its process for [redacted] listed in System Security Plans for outdated or inaccurate [redacted] as part of the agency's annual System Security Plan reviews in order to ensure the consistent maintenance of a comprehensive and accurate inventory of [redacted].

Management Response. We concur. The SEC has developed and [redacted]. This process is further detailed in [redacted]. The SEC will evaluate these procedures for completeness and, if necessary, add steps to ensure the consistent maintenance of a comprehensive and accurate inventory of [redacted]. Management's complete response is reprinted in Appendix IV.

Kearney's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 2: Develop, document, and implement a process for documenting the results of privacy risk assessments into the agency's [redacted].

Management Response. We concur. OIT currently utilizes the existing process documented in [redacted], to record Plan of Action and Milestones (POA&M) resulting from privacy risk assessments into the agency's [redacted] and track through closure. This Operating Procedure will be updated to specifically define its applicability to privacy POA&Ms. The SEC will also include the Privacy Assessment Report in the agency's [redacted]. Management's complete response is reprinted in Appendix IV.

Kearney's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 3: Develop and implement a process to [redacted].

Management Response. We concur. In accordance with *FISMA* and SECR 24-04, *Information Technology Security Program*, Information System Owners perform annual system documentation reviews, which include [redacted]. OIT will refine its process to require outdated or inaccurate [redacted] so that [redacted].
Management's complete response is reprinted in Appendix IV.

Kearney's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Domain #2: SCRM

Unlike FY 2021, the *FY 2022 IG FISMA Reporting Metrics* include the SCRM domain for the Identify function rating. NIST SP 800-161, Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, defines cybersecurity supply chain risk management as a "systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures." In addition, according to the *FY 2021 IG FISMA Reporting Metrics*, SCRM activities include ensuring that products, system components, systems, and services of external providers adhere to the agency's defined supply chain requirements.

Kearney assessed the SEC's supply chain risk management program and determined that the program's assessed maturity level is Level 1: *Ad Hoc*, meaning the SEC's policies and procedures for SCRM are not formalized and SCRM activities are performed in an ad hoc, reactive manner.

Current-Year Findings: In the FY 2021 FISMA report, Kearney did not issue a finding for SCRM; however, we presented the SEC with an Other Matter regarding the agency's SCRM program. Kearney has identified additional opportunities for the agency to mature its SCRM program.

In addition to the prior-year matter, Kearney identified a new improvement opportunity related to the agency's supply chain risk management requirements for external providers.

The SEC did not define policies and procedures to ensure adherence to its cybersecurity and supply chain risk management requirements for external providers. The *FY 2022 IG FISMA Reporting Metrics* measure the extent to which agencies define policies and procedures to ensure adherence to their cybersecurity and supply chain risk management requirements for external providers. Additionally, NIST SP 800-53, Rev.5, SR-2, states that the organization should develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: organization-defined systems, system components, or system services; review and update the supply chain risk management plan, to address threat, organizational or environmental changes; and protect the supply chain risk management plan from unauthorized disclosure and modification. Further, NIST SP 800-53, Rev.5, SR-3, states that the organization should document the selected and implemented supply chain processes and controls in the security and privacy plans or supply chain risk management plan.

While the SEC has finalized its Information and Communication Technology Supply Chain Vendor Risk Management Strategy, the SEC did not define policies and procedures to ensure adherence to its cybersecurity and supply chain risk management requirements for external providers.

This occurred, in part, because the SEC Executive Committee is in the process of developing an agency-wide supply chain risk strategy that will define policies and procedures to ensure adherence to its cybersecurity and supply chain risk management requirements for external providers. Further, the SCRM requirements for NIST SP 800-53, Rev. 5, went into effect in September 2021, and the SEC is working on implementing the newly introduced requirements.

Without defined policies and procedures to ensure adherence to its cybersecurity and supply chain risk management requirements for external providers, the SEC may experience unexpected, adverse effects or unintended changes to the supply chain and SEC infrastructure. In addition, without defined policies and procedures, the agency may experience unexpected, adverse effects to its relationship with external providers, such as unsatisfactory fulfillment of requirements.

Recommendation, Management's Response, and Evaluation of Management's Response

Additionally, Kearney & Company, P.C. recommends that the U.S. Securities and Exchange Commission's Office of Information Technology:

Recommendation 4: Develop and define policies and procedures to ensure adherence to its cybersecurity and supply chain risk management requirements for external providers within the agency's Supply Chain Risk Management Strategy.

> **Management Response.** We concur. The SEC currently has existing processes or controls in place that mitigate certain supply chain risks and cybersecurity risks. OIT will continue its work to develop and implement supply chain risk management requirements for external providers in accordance with an *SEC Information and Communications Technology Supply Chain Risk Management Policy*. Management's complete response is reprinted in Appendix IV.
>
> **Kearney's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Domain #3: Configuration Management

The *FY 2022 IG FISMA Reporting Metrics*, in accordance with NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, dated August 2011, consider configuration management an important process for establishing and maintaining secure information system configurations, in addition to providing critical support for managing security risks in systems. Configuration management activities include developing baseline configurations, establishing a configuration change control process, implementing a configuration monitoring and reporting process, and implementing a Vulnerability Disclosure Policy. NIST SP 800-53, Rev. 5, CM-2, "Baseline Configuration," requires that organizations develop, document, and maintain, under configuration control, a current baseline configuration of the system, as well as review and update the baseline configuration of the system. In addition, NIST SP 800-53, Rev. 5, CM-3 (f), "Configuration Change Control," states that organizations should monitor and review activities associated with configuration-controlled changes to the information system. Further, NIST SP 800-53, Rev. 5, SI-2, "Flaw Remediation," states that organizations should identify, report, and correct system flaws.

Kearney assessed the SEC's configuration management program and determined that the program's assessed maturity level is Level 2: *Defined*, meaning the SEC formalized and documented configuration management policies, procedures, and strategies, but it did not consistently implement them. The SEC's assessed maturity remained at Level 2: *Defined* between FYs 2021 and 2022, as it has not fully implemented the recommendations identified in prior years; therefore, certain previously identified conditions still exist.

Prior-Year Findings: Specifically, in the FY 2021 FISMA evaluation, the OIG determined that the SEC did not:

- Develop, document, or implement a formal process to consistently capture and share lessons learned on the effectiveness of its configuration baseline program and make updates, as necessary.

Similarly, Kearney determined that the weaknesses within the SEC's configuration management program identified during the FY 2021 FISMA evaluation remained present in FY 2022, as listed below:

- The SEC did not consistently utilize lessons learned to make improvements to its secure configuration policies and procedures.

This occurred, in part, because the agency was still working towards implementing lessons learned into its configuration management procedures through the continued development of its lessons learned operating procedures.

Kearney is not making any new recommendations in relation to the prior-year findings noted above, as the SEC is working to address the prior-year FISMA recommendations. See **Appendix II: Open FISMA Recommendations**.

Current-Year Findings: Kearney has identified additional opportunities for the agency to mature its configuration management program.

In addition to the prior-year findings, Kearney identified new weaknesses related to the SEC's [redacted] and the [redacted].

The SEC did not consistently deploy and maintain [redacted]. The *FY 2022 IG FISMA Reporting Metrics* measure the extent to which agencies consistently deploy and maintain secure configuration settings for their workstations. Additionally, NIST SP 800-53, Rev. 5, CM-6, states that each organization should implement its configuration settings and "identify, document, and approve any deviations from established configuration settings." Further, NIST Cybersecurity Framework, Control PR.IP-1, states: "A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles."

The SEC defined its policies and procedures for managing and remediating configuration compliance deviations. Additionally, the agency targets a self-defined goal of 90 percent configuration compliance for its information systems. However, the SEC did not consistently [redacted].

This occurred, in part, because the SEC did not [redacted].

Without the [redacted], the agency risks the employment and operation of systems that do not adhere to organizational operational requirements.

The SEC did not consistently implement its policies, procedures, and processes for [redacted]. The *FY 2022 IG FISMA Reporting Metrics* measure the extent to which agencies consistently implement policies, procedures, and processes for flaw remediation and consistently patch critical vulnerabilities within 30 days. Additionally, NIST SP 800-53, Rev. 5, SI-2, states that the organization should "incorporate flaw remediation into the organizational configuration management process" and that the organization should have "organization-defined time periods for updating security relevant software and firmware." NIST SP 800-53, Rev. 5, SI-2, also notes that organizations should "address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified." The *OIT Vulnerability Management Policy* requires critical vulnerabilities to be remediated in 45 days, high vulnerabilities in 60 days, and medium vulnerabilities in 90 days. Finally, the *OIT Vulnerability Management Policy* requires that exploitable critical, high, and medium vulnerabilities must be remediated in 15 days.

The SEC developed, documented, and disseminated its policies, procedures, and processes for flaw remediation. However, the agency did not [redacted]. Specifically, [redacted].

This occurred, in part, because the SEC did not implement its process [redacted]. Specifically, the agency [redacted]

Without the [redacted], the SEC risks [redacted].

Recommendations, Management's Response, and Evaluation of Management's Response

To mature the U.S. Securities and Exchange Commission's configuration management program, Kearney & Company, P.C. recommends that the Office of Information Technology continue to work to close prior-year recommendations. See **Appendix II: Open FISMA Recommendations**.

Additionally, Kearney & Company, P.C. recommends that the U.S. Securities and Exchange Commission's Office of Information Technology:

Recommendation 5: Develop and implement a process to deploy [redacted].

> **Management Response.** We concur on the importance of having a process of [redacted]. OIT currently includes [redacted]. OIT will review its policies and procedures and make applicable updates to ensure processes are in place for [redacted]. Specific to this recommendation, OIT will [redacted]. Management's complete response is reprinted in Appendix IV.

Kearney's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 6: Implement the defined processes for [redacted].

Management Response. We concur. OIT will update the [redacted]. OIT will apply these more specific actions to the agency's [redacted]. Management's complete response is reprinted in Appendix IV.

Kearney's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Domain #4: Identity and Access Management

The *FY 2022 IG FISMA Reporting Metrics*, in accordance with the NIST Cybersecurity Framework, require agencies to establish an identity and access management program that limits access to physical and logical assets and associated facilities to authorized users, processes, and devices, which is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. NIST SP 800-53, Rev. 5, AC-1, "Access Control Policy and Procedures," and IA-1, "Identification and Authentication Policy and Procedures," require organizations to develop, document, and disseminate an access control policy and identification and authentication policy that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The SEC employs an identity and access management program to ensure that only authorized individuals have access to SEC information systems; users are restricted to authorized transactions, functions, and information; access is assigned according to the principles of separation of duties and least privilege; and users are individually accountable for their actions.

Furthermore, an identification and authentication process confirms the identity of users before granting access to SEC information and information systems. The continued development of a strong identity and access management program may decrease the risk of unauthorized access to the SEC's network, information systems, and data.

Kearney assessed the SEC's identity and access management program and determined that the program's assessed maturity level is Level 2: *Defined*, meaning the SEC formalized and documented identity and access management policies, procedures, and strategies, but it did not consistently implement them. While the agency continued to make improvements, the SEC's assessed maturity remained at Level 2: *Defined* between FYs 2021 and 2022, as it has not fully implemented the recommendations identified in prior years; therefore, certain previously identified conditions still exist.

Prior-Year Findings: Specifically, in the FY 2017 FISMA audit, the OIG identified that the SEC did not:

- [redacted].

Similarly, Kearney determined that the weakness within the SEC's identity and access management program identified during the FY 2017 FISMA audit remained present in FY 2022, as listed below:

- [redacted].

This control weakness occurred, in part, because the ongoing work-from-home posture at the SEC due to the Coronavirus Disease 2019 pandemic caused delays in remediating the agency's existing Corrective Action Plan for implementing strong authentication for its users. In the meantime, the agency continues to enforce mandatory multi-factor authentication for all staff accessing the SEC network through remote access and OIT has a pilot underway for the use of [redacted] as a [redacted] alternative for multi-factor authentication at local workstations.

Current-Year Findings: Kearney has identified additional opportunities for the agency to mature its identity and access management program. See the findings detailed below.

In addition to the prior-year findings, Kearney identified a new weakness related to the SEC's completion of [redacted] for information systems.

The SEC did not consistently complete [redacted] for its information systems. The *FY 2022 IG FISMA Reporting Metrics* measure the extent to which agencies consistently complete processes for provisioning, managing, and reviewing privileged accounts. Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed. Additionally, NIST SP 800-53, Rev. 5, AC-6, states that organizations should "employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks." Further, NIST SP 800-53, Rev. 5, AC-5, notes that organizations should identify and document organization-defined duties of individuals requiring separation, as well as define system access authorizations to support separation of duties. Finally, the SEC's Identity Credential and Access Management Strategy requires the agency to consistently complete user access recertifications for its information systems on a biannual basis.

The SEC defined its policies and procedures for the completion of [redacted] for its sampled systems. However, the agency did not [redacted].

This occurred, in part, because the agency did not develop and implement a process, including the timelines, for [redacted]. Specifically, the [redacted] system was previously a General Support System (GSS) component but had moved to the cloud and, thus, became FISMA-reportable. As a result, [redacted].

Without the [redacted], the SEC may be unable to employ [redacted]. In addition, the agency risks the [redacted].

Recommendation, Management's Response, and Evaluation of Management's Response

To mature the U.S. Securities and Exchange Commission's identity and access management program, Kearney & Company, P.C. recommends that the Office of Information Technology continue to work to close prior-year recommendations. See **Appendix II: Open FISMA Recommendations**.

Additionally, Kearney & Company, P.C. recommends that the U.S. Securities and Exchange Commission's Office of Information Technology:

Recommendation 7: Develop and implement a process, including the timelines, [redacted].

> **Management Response.** We concur. OIT will update [redacted]. This process is applicable to all systems, including cloud systems. The SEC will then follow the procedures for [redacted]. Management's complete response is reprinted in Appendix IV.
>
> **Kearney's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Domain #5: Data Protection and Privacy

The NIST Cybersecurity Framework requires agencies to manage information and records (data) consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. In pursuit of its mission to protect investors, the SEC collects sensitive, non-public information that may include Personally Identifiable Information (PII). The collection of sensitive PII requires the SEC to take additional precautions to prevent accidental disclosure, such as encrypting sensitive data at rest, as well as in transit. The collection of sensitive PII also requires the SEC to notify the public of why information is collected, its intended use, with whom it will be shared, and how the information will be protected.

Kearney assessed the SEC's data protection and privacy program and determined that the program's assessed maturity level is Level 3: *Consistently Implemented*, meaning the SEC formalized and consistently implemented privacy policies, procedures, and strategies for data protection and privacy, but its quantitative and qualitative effectiveness measures were lacking. The SEC's assessed maturity for data protection and privacy remained at Level 3: *Consistently Implemented* between FYs 2021 and 2022.

Current-Year Findings: Kearney has identified additional opportunities for the agency to mature its data protection and privacy program. See the finding detailed below.

The SEC did not [redacted]. The *FY 2022 IG FISMA Reporting Metrics* measure the extent to which agencies manage and measure the effectiveness of their data exfiltration and enhanced network defense processes. Further, the reporting metrics measure the extent to which agencies "measured the effectiveness of its data exfiltration and enhanced network defenses by conducting exfiltration exercises." Additionally, NIST SP 800-53, Rev. 5, SC-7(10), notes that prevention of exfiltration applies to both the intentional and unintentional exfiltration of information. Techniques used to prevent the exfiltration of information from systems may be implemented at internal endpoints, external boundaries, and across managed interfaces and include adherence to protocol formats, monitoring for beaconing activity from systems, disconnecting external network interfaces except when explicitly needed, employing traffic profile analysis to detect deviations from the volume and types of traffic expected, sending call-backs to command and control centers, conducting penetration testing, monitoring for steganography, disassembling and reassembling packet headers, and using data loss and data leakage prevention tools.

While the SEC consistently implemented its defined policies and procedures for enhanced network defense processes, the agency did not [redacted]. Specifically, [redacted].

This occurred, in part, because the SEC did not [redacted]. According to OIT, this occurred, to a certain extent, due to competing priorities. The SEC was unable to [redacted]. Previously, [redacted] were included as part of the [redacted].

Without the completion of [redacted], the agency may be unable to manage and measure [redacted]. In addition, if the SEC does not [redacted].

The SEC did [redacted]. The *FY 2022 IG FISMA Reporting Metrics* measure the extent to which agencies document security controls to prevent data exfiltration and enhance network defenses. The reporting metrics further measure the extent to which agencies monitor their DNS infrastructure for potential tampering, in accordance with their ISCM Strategies. Additionally, NIST SP 800-53, Rev. 5, SI-4, states that system monitoring includes external and internal monitoring. Specifically, external monitoring includes the observation of events occurring at external interfaces to the system, while internal monitoring comprises the observation of events occurring within the system. NIST SP 800-53, Rev. 5, SI-4, further requires organizations to monitor systems by observing audit activities in real-time or by observing other system aspects, such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capabilities are achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.

While the SEC consistently implemented its policies and procedures for data exfiltration prevention and enhanced network defenses, the agency did not [redacted].

This occurred, in part, because the SEC did not [redacted].

Without the [redacted].

The SEC did not consistently [redacted]. The *FY 2022 IG FISMA Reporting Metrics* measure the extent to which agencies have consistently implemented the encryption of data at rest for its information systems. Additionally NIST SP 800-53, Rev. 5, SC-28, states: "… the focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information… Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms…" Furthermore, OMB M-22-09, *Federal Zero Trust Strategy*, notes: "Executive Order 14028 directs agencies to use encryption to protect data at rest."

The SEC defined and communicated tailored policies and procedures for the protection of PII and other sensitive data based upon its classification and sensitivity. However, the SEC did not [redacted].

This occurred, in part, because the SEC did not [redacted].

Without the consistent implementation of [redacted], the agency risks the [redacted].

Recommendations, Management's Response, and Evaluation of Management's Response

Kearney & Company, P.C. recommends that the U.S. Securities and Exchange Commission's Office of Information Technology:

Recommendation 8: Develop a process for conducting [redacted] in order to manage and measure the effectiveness of the agency's [redacted].

> **Management Response.** We concur. The SEC currently performs activities to measure the effectiveness of [redacted]. OIT will also develop a process and perform a [redacted]. Management's complete response is reprinted in Appendix IV.
>
> **Kearney's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 9: Document and integrate [redacted].

> **Management Response.** We concur. OIT will incorporate the existing [redacted].
>
> **Kearney's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the

action taken.

Recommendation 10: Develop a process to consistently implement [redacted].

Management Response. We concur. [redacted]. Management's complete response is reprinted in Appendix IV.

Kearney's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Domain #6: Security Training

FISMA requires agencies to establish an information security program that includes security awareness training. Such training informs personnel, including contractors, of information security risks associated with their activities, as well as their responsibilities for complying with agency policies and procedures. NIST SP 800-181, *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework*, dated August 2017, provides guidance on a superset of cybersecurity knowledge, skills, and abilities and tasks for each work role. The *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework* supports consistent organizational and sector communication for cybersecurity education, training, and workforce development. NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, dated October 2003, mandates that organizations monitor their information security training program for compliance and effectiveness and that failure to encourage IT security training puts an agency at great risk because the security of agency resources is as much a human issue as it is a technology concern. Lastly, NIST SP 800-53, Rev. 5, AT-3, "Role-Based Training," requires that Federal agencies provide role-based security training to personnel with assigned security roles and responsibilities before authorizing access or performing assigned duties.

Kearney assessed the SEC's security training program and determined that the program's assessed maturity level is Level 2: *Defined*, meaning the SEC formalized and documented security training policies, procedures, and strategies, but it did not consistently implement them. Finally, Kearney noted that there was a significant decrease in the overall Security Training domain rating (from *Optimized* in FY 2021 to *Defined* in FY 2022). The OIG's independent assessor determined that this decline was primarily due to changes in the methodology for the FY 2022 assessment.

Prior-Year Findings: Specifically, in the FY 2020 FISMA evaluation, the OIG determined that the SEC did not:

- Define and implement a process to incorporate results from the assessments of knowledge, skills, and abilities into the Security Training Strategy.

Similarly, Kearney determined that the weaknesses with the SEC's security training program identified during the FY 2020 FISMA evaluation remained present in FY 2022 as listed below:

- The SEC did not utilize the results from its assessments of knowledge, skills, and abilities to update the agency's Security Training Strategy.

This control weakness occurred, in part, because the agency was in the process of developing a capstone quiz at the end of its Privacy Information Security Awareness (PISA) training to identify participant comprehension and knowledge, skills, and abilities to improve the PISA training from year to year.

Kearney is not making any new recommendations in this area, as the SEC is still working to resolve all prior-year FISMA recommendations. See **Appendix II: Open FISMA Recommendations**.

Domain #7: ISCM

The *FY 2021 IG FISMA Reporting Metrics* require agencies to establish information security programs that include ISCM. ISCM refers to the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The output of a strategically designed and well-managed organization-wide ISCM program can be used to maintain a system's authorization to operate and keep required system information and data up to date on an ongoing basis. According to NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, dated September 2011, organizations should take steps to establish, implement, and maintain an ISCM program, including defining an ISCM strategy, analyzing and reporting findings, and reviewing and updating the ISCM strategy and program, as necessary.

Kearney assessed the SEC's ISCM program and determined that the program's assessed maturity level was Level 3: *Consistently Implemented*, consistent with FY 2021, meaning the SEC formalized and consistently implemented its continuous monitoring policies, procedures, and strategies for ongoing authorization, but its quantitative and qualitative effectiveness measures were lacking.

Current-Year Finding: Kearney has identified additional opportunities for the agency to further mature its ISCM program. See the finding detailed below.

The SEC did not transition to ongoing control and system authorization. The *FY 2022 IG FISMA Reporting Metrics* measure the extent to which agencies transitioned to ongoing control and system authorization through the implementation of their continuous monitoring policies and strategy. Additionally, NIST SP 800-137, Section 3.1 states that effective ISCM begins with the development of a strategy that addresses ISCM requirements and activities at each organizational tier (organization, mission/business processes, and information systems). Each tier monitors security metrics and assesses security control effectiveness with established monitoring and assessment frequencies and status reports customized to support tier-specific decision-making. Policies, procedures, tools, and templates that are implemented from Tiers 1 and 2, or that are managed in accordance with guidance from Tiers 1 and 2, best support shared use of data within and across tiers. The lower tiers may require information in addition to that required at higher tiers and, hence, develop tier-specific strategies that are consistent with those at higher tiers and still sufficient to address local tier requirements for decision-making. Depending on the organization, there may be overlap in the tasks and activities conducted at each tier. Finally, the DHS Continuous Diagnostic and Mitigation (CDM) program was implemented with the goal to fortify cybersecurity of Government networks and systems by providing Federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis.

The SEC consistently implemented its ISCM policies and strategy at the organization, mission/business process, and information system levels. However, the agency did not transition to ongoing control and system authorization through the implementation of its continuous monitoring policies and strategies. Specifically, the agency did not [redacted].

This occurred, in part, because the SEC planned to transition to ongoing control and system authorization using [redacted].

[redacted].

Recommendation, Management's Response, and Evaluation of Management's Response

Kearney & Company, P.C. recommends that the U.S. Securities and Exchange Commission's Office of Information Technology:

Recommendation 11: Complete implementation of the Continuous Diagnostic and Mitigation Dashboard as a Service in coordination with Department of Homeland Security/Cybersecurity and Infrastructure Security Agency to better support existing ongoing control activities.

> **Management Response.** We concur. OIT will coordinate with the Department of Homeland Security/Cybersecurity & Infrastructure Security Agency to implement the Continuous Diagnostic and Mitigation Dashboard as a Service. Management's complete response is reprinted in Appendix IV.
>
> **Kearney's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Domain #8: Incident Response

FISMA requires agencies to develop, document, and implement organization-wide information security programs that include procedures for detecting, reporting, and responding to security incidents, including mitigating the risks of such incidents before substantial damage occurs. According to NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide*, dated August 2012, key phases in the incident response process are: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity.

Kearney assessed the SEC's incident response program and determined that the program's assessed maturity level is Level 4: *Managed and Measurable*, meaning the SEC formalized strategies for collecting quantitative and qualitative effectiveness measures to promote continuous improvement. The agency's assessed maturity remained consistent at Level 4: *Managed and Measurable* between FYs 2021 and 2022. While the agency's incident response program was effective, we identified additional areas for improvement.

Current-Year Finding: Kearney has identified opportunities for the agency to further mature its incident response program. See the finding detailed below.

The SEC did not consistently capture and share formal lessons learned on the effectiveness of its incident handling policies and procedures. The *FY 2022 IG FISMA Reporting Metrics* measure the extent to which agencies consistently capture and share lessons learned on the effectiveness of their incident handling policies and procedures. Additionally, NIST SP 800-61, Rev. 2, notes that organizations should use the lessons learned process to gain value from incidents. The guidance further states: "After a major incident has been handled, the organization should hold a lessons learned meeting to review the effectiveness of the incident handling process and identify necessary improvements to existing security controls and practices."

The SEC developed a detailed out-brief process for reviewing completed incident investigations. However, the agency did not have a process to consistently capture or share formal lessons learned on the effectiveness of its incident handling policies and procedures, nor make updates, as necessary.

This occurred, in part, because the SEC did not have a process to consistently capture and share formal lessons learned on the effectiveness of its incident handling policies and procedures. Specifically, the agency is still working to develop, document, and implement an overall process for consistently capturing and sharing formal lessons learned on the effectiveness of its incident handling policies and procedures.

Without the consistent capturing and sharing of formal lessons learned on the effectiveness of incident handling policies and procedures, the agency risks not adapting its incident response program based on previous and current cybersecurity activities or the ever-evolving cybersecurity landscape.

Recommendation, Management's Response, and Evaluation of Management's Response

Kearney & Company, P.C. recommends that the U.S. Securities and Exchange Commission's Office of Information Technology:

Recommendation 12: Develop, document, and implement a formal process for consistently capturing and sharing formal lessons learned on the effectiveness of incident handling policies and procedures and make updates, as necessary.

> **Management Response.** We concur. As part of prior year corrective actions 570-3, 4 and 7, OIT is developing a lessons learned operating procedure to ensure consistency in capturing and sharing lessons learned. Once the operating procedure is finalized, incident-handling lessons learned will be performed in accordance with the procedure. Management's complete response is reprinted in Appendix IV.
>
> **Kearney's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Domain #9: Contingency Planning

FISMA requires agencies to develop, document, and implement plans and procedures to ensure continuity of operations for information systems supporting the operations and assets of the organizations. Because information system resources are essential to an organization's success, it is critical that systems are able to operate effectively without excessive interruption.

Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and efficiently as possible following a disaster. NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, dated May 2010, states that contingency planning activities include developing the planning policy, creating contingency strategies, maintaining contingency plans, conducting Business Impact Analyses (BIA), testing contingency plans, and conducting exercises. In addition, NIST SP 800-53, Rev. 5, CP-4, "Contingency Plan Testing and Exercises," requires organizations to perform periodic testing of contingency plans to determine the effectiveness and organizational readiness to execute the plans. Further, NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, CP-1, "Contingency Planning Policies and Procedures, Supplemental Information and Communications Technology (ICT) Supply Chain Risk Management Guidance," dated May 2022, states that organizations should integrate ICT supply chain concerns into their contingency planning policies.

Kearney assessed the SEC's contingency planning program and determined that the program's maturity level is Level 3: *Consistently Implemented*, meaning the SEC consistently implemented its continuous monitoring policies, procedures, and strategies for its contingency planning processes, but quantitative and qualitative effectiveness measures were lacking. The SEC decreased in the overall Contingency Planning domain rating (from Level 4: *Managed and Measurable* in FY 2021 to Level 3: *Consistently Implemented* in FY 2022). The OIG's independent assessor determined that this decline was due, in part, to changes in the methodology for the FY 2022 assessment, which included fewer metrics for contingency planning.

Prior-Year Findings: Specifically, in the FY 2021 FISMA evaluation, Kearney determined that the SEC did not:

- Develop, document, or implement a process to consistently utilize automated testing for information system contingency plan efforts, [redacted].

Similarly, Kearney determined that the weakness with the SEC's Contingency Planning program identified during the FY 2021 FISMA evaluation remained present in FY 2022, as listed below:

- While the SEC conducts testing of system contingency planning efforts, the agency did not implement automated testing capabilities for these tests.

This control weakness occurred, in part, because the agency is currently still developing a process for consistently utilizing automated testing for system contingency plan testing and is targeting a completion date of December 20, 2022.

Current-Year Finding: Kearney has identified additional opportunities for the agency to further mature its contingency planning program. See the finding detailed below.

The SEC did not consistently complete BIAs for its information systems. The *FY 2022 IG FISMA Reporting Metrics* measure the extent to which agencies consistently complete BIAs for their information systems. Additionally, NIST SP 800-53, Rev. 5, CP-2, states that the organization should "develop a contingency plan for the system that: identifies essential mission and business functions and associated contingency requirements; provides recovery objectives, restoration priorities, and metrics; addresses contingency roles, responsibilities, and assigned individuals with contact information; addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure; addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; addresses the sharing of contingency information; and undergoes review and approval by organization-defined personnel or roles." Further, NIST SP 800-53, Rev. 5, RA-9, states that the organization should "identify critical system components and functions by performing a criticality analysis for organization-defined systems, system components, or system services at organization-defined decision points in the system development life cycle."

The SEC defined its policies, procedures, and processes for completing BIAs for its information systems. However, the agency did not consistently complete BIAs for its information systems, as the BIA for one of eight (12.5 percent) sampled systems [redacted] was incomplete during the evaluation scope period.

This occurred, in part, because the SEC did not take steps to ensure that BIAs for its information systems changing to a cloud service provider were updated to reflect their current environment. Specifically, [redacted] was previously a GSS component; however, in February 2021, it moved to the cloud and became an independent system. As a result, the [redacted] system now requires consistent completion of BIAs. Due to the updated state of the [redacted] system, OIT did not complete its BIA prior to system authorization.

Without consistent completion of BIAs for its information systems, the agency risks adverse effects to the continuity of operations for organization mission and business functions.

Recommendation, Management's Response, and Evaluation of Management's Response

Kearney & Company, P.C. recommends that the U.S. Securities and Exchange Commission's Office of Information Technology:

Recommendation 13: Develop steps to ensure that Business Impact Analyses for information systems, including information systems that have moved to a cloud service provider, are consistently completed as part of the system authorization process.

Management Response. We concur. OIT performs a FISMA-reportable inventory review twice a year to ensure system data is up-to-date. At the time of the assessment, [redacted] was identified as a GSS tool and later changed to a cloud service provider. A Business Impact Analysis (BIA) was completed, signed, and provided to OIG after the evaluation scope. OIT will update its process to include automatic notification of information system type changes to ensure BIAs for information systems that have moved to a cloud service provider are consistently completed as part of the system authorization process. Management's complete response is reprinted in Appendix IV.

Kearney's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Overall Conclusion

The SEC has made progress in improving its information security program by institutionalizing the use of advanced risk management technologies; developing a standard hardware taxonomy across the agency; and updating relevant components of the agency's interconnection inventory. While the SEC made program improvements, the agency faced challenges with: 1) maintaining a comprehensive and accurate [redacted]; 2) documenting the results of privacy risk assessments; 3) maintaining a complete [redacted]; 4) defining policies and procedures for cybersecurity and supply chain risk management requirements for external providers; 5) deploying and maintaining [redacted]; 6) implementing policies, procedures, and processes for [redacted]; 7) completing [redacted] for information systems; 8) managing and measuring the effectiveness of [redacted]; 9) monitoring [redacted]; 10) implementing [redacted] for information systems; 11) transitioning to [redacted]; 12) integrating formal lessons learned on the effectiveness of incident handling policies and procedures; and 13) completing BIAs for its information systems.

As a result, the OIG's independent assessor, Kearney, determined that the SEC's information security program did not meet OMB's definition of "effective." Kearney also noted that there was a significant decrease in both the overall Security Training domain rating (from *Optimized* in FY 2021 to *Defined* in FY 2022) and the Contingency Planning domain rating (from *Managed and Measurable* in FY 2021 to *Consistently Implemented* in FY 2022). We determined that these decreases were primarily due to changes in the methodology for the FY 2022 assessment. Specifically, the FY 2022 assessment included fewer metrics overall than the FY 2021 evaluation.

Appendix I: Scope and Methodology

Kearney conducted this independent evaluation of the SEC's information security program and practices under CIGIE's *Quality Standards for Inspection and Evaluation.* Those standards require that we plan and perform the evaluation to obtain sufficient, competent, and relevant evidence to provide a reasonable basis for our findings, conclusions, and recommendations based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives. Our evaluation included inquiries, observations, and inspection of SEC documents and records, as well as direct testing of controls.

Scope: Our overall objective was to assess the SEC's implementation of FISMA and respond to the *FY 2022 IG FISMA Reporting Metrics*. As required by FISMA, we assessed the SEC's information security posture based on guidance issued by OMB, DHS, and NIST.

The evaluation covered the period between October 1, 2021 and March 31, 2022 and addressed the following nine domains specified in the *FY 2022 IG FISMA Metrics*:

- Risk Management
- Supply Chain Risk Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Training
- Information Security Continuous Monitoring
- Incident Response
- Contingency Planning.

Methodology: To assess the effectiveness and maturity of the SEC's information security program, focusing on the 20 core metrics identified in the *FY 2022 IG FISMA Reporting Metrics*, Kearney judgmentally selected and reviewed a non-statistical sample of eight information systems from the SEC's April 4, 2022 inventory of 99 (or about 8 percent) FISMA-reportable information systems. To select the sample, Kearney used the following criteria:

- Systems that were not previously tested in the prior three years
- Systems that were categorized as "moderate" or "high" under FIPS PUB 199
- Systems that contain sensitive and confidential information, including PII data
- Systems classified as an HVA.

The sample consisted of the internally and externally hosted systems shown in **TABLE 3**. To assess system security controls, Kearney reviewed the security assessment packages for the eight FISMA-reportable systems. In addition, to address the requirements of the *FY 2022 IG FISMA Reporting Metrics* for the Identity and Access Management and Incident Response domains, we judgmentally selected and reviewed a non-statistical sample of controls related to those domains. This included a random sample of 45 of 1,030 (about 4 percent) service accounts to assess the agency's service account maintenance process and a random sample of eight of 44 (about 18 percent) security incidents to evaluate the agency's incident handling process. Because sampled items were non-statistical, Kearney did not project our results and conclusions to the total user population or measure overall prevalence.

TABLE 3. [redacted]

System	System Description	FIPS PUB 199 Categorization	Operated By
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

REDACTED FOR PUBLIC RELEASE

System	System Description	FIPS PUB 199 Categorization	Operated By
	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]

Source: [redacted] eGRC tool, SEC system of record

To rate the maturity level of the SEC's information security program and functional areas, Kearney used the scoring methodology defined in the *FY 2021 IG FISMA Reporting Metrics*. We interviewed key personnel, including staff from OIT's Security and Privacy Compliance Group and Security Design and Engineering Branch. Kearney also examined documents and records relevant to the SEC's information security program, including applicable Federal laws and guidance; SEC administrative regulations, policies, and procedures; system-level documents; and reports. As discussed throughout this report, these included, but were not limited to, the following:

- FISMA (PL 113-283)
- E-Government Act of 2002 (PL 107-347)
- Applicable OMB guidance, including OMB Circular A-130, *Managing Federal Information as a Strategic Resource*, dated July 2016, and OMB M-16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*, dated October 2015
- Various NIST SPs
- SEC Administrative Regulation 24-04, Rev. 4, *Information Technology Security Program*
- SEC OIT policies.

Finally, Kearney reviewed the SEC's progress toward implementing recommendations from prior FISMA reports.

Internal Controls: Consistent with our evaluation objective, we did not assess OIT's overall management control structure. Instead, Kearney reviewed the SEC's controls specific to the *FY 2022 IG FISMA Reporting Metrics*. To understand OIT's management controls pertaining to its policies, procedures, and methods of operation, we relied on information requested from and supplied by OIT staff and information from interviews with OIT personnel. Kearney noted that the SEC generally complied with applicable FISMA and SEC policies and procedures, except as identified in this report. Our recommendations, if implemented, should address the areas of improvement we identified, as well as assist the SEC's information security program reach the next maturity level.

Data Reliability: The Government Accountability Office's (GAO) *Assessing Data Reliability* (GAO-20-283G), dated December 2019, states that reliability of data means that data is applicable for audit purpose and are sufficiently complete and accurate. Data primarily pertains to information that is entered, processed, or maintained in a data system and is generally organized in, or derived from, structured computer files. Furthermore, GAO-20-283G defines "applicability for audit purpose," "completeness," and "accuracy" as follows:

- "Applicability for audit purpose" refers to whether the data, as collected, are valid measure of the underlying concepts being addressed in the audit's research objectives
- "Completeness" refers to the extent that relevant data records and fields are present and sufficiently populated
- "Accuracy" refers to the extent that recorded data reflects the actual underlying information.

Kearney used the SEC's eGRC tool as a data source for obtaining documentation and reports related to the sampled systems and FISMA-reportable information systems inventory. We also used the SEC's training management system. Kearney performed data reliability, completeness, and accuracy testing, in part, by comparing computer-processed information to testimonial evidence obtained from Information System Owners and by comparing system outputs for consistency. As a result of these tests, we determined that the computer-processed data we reviewed was sufficiently reliable to support our conclusions.

Prior Coverage: As of May 25, 2022, the SEC took corrective action sufficient to close 12 recommendations from prior-year FISMA reports within FY 2022. Specifically, within FY 2022, the SEC took actions to close two of four open recommendations from the OIG's audit of the SEC's compliance with FISMA for FY 2017 (FY 2017 FISMA audit), dated March 30, 2018; two of three open recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2018 (FY 2018 FISMA evaluation), dated December 12, 2018; four of four open recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2019 (FY 2019 FISMA evaluation), dated December 18, 2019; three of five open recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2020 (FY 2020 FISMA evaluation), dated December 21, 2020; and one of seven open recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2021 (FY 2021 FISMA evaluation), dated December 21, 2021. Although OIT addressed these recommendations, as we noted in this report, areas for improvement still exist. **Appendix II: Open FISMA Recommendations** lists all open OIG recommendations from prior FISMA audits and evaluations.

SEC OIG audit and evaluation reports, including the FYs 2017, 2018, 2019, 2020, and 2021 FISMA reports, can be accessed at: https://www.sec.gov/oig.

Appendix II: Open FISMA Recommendations

TABLE 4 lists all FISMA recommendations that remain open from prior FISMA audit and evaluations as of May 25, 2022.

TABLE 4. Open FISMA Recommendations

Domain and Function Area	Open Recommendations
FY 2017	
Configuration Management (Identify)	**Recommendation 8:** Develop, review, and approve secure baselines for all systems included in the U.S. Securities and Exchange Commission's [redacted].
Information Access Management (Identify)	**Recommendation 12:** [redacted].
FY 2018	
Configuration Management (Identify)	**Recommendation 1:** Update configuration management procedures to require that [redacted]
FY 2020	
Risk Management (Identify)	**Recommendation 1:** Develop and document: a) agency requirements for applying security and operating system updates to mobile devices in an organizationally defined timeframe; [redacted].
Security Training (Protect)	**Recommendation 6:** Define and implement a process to incorporate results from the assessments of knowledge, skills, and abilities into the security training strategy.
FY 2021	
Risk Management (Identify)	**Recommendation 1:** Develop, document, and implement a process for consistently implementing [redacted] within the agency's [redacted].
	Recommendation 2: Develop, document, and implement a process to clearly define requirements for consistently completing and maintaining Federal Information Processing Standards Publication 199 categorization worksheets for all system types.
	Recommendation 3: Develop, document, and implement a formal process to consistently capture and share lessons learned on the effectiveness of its cybersecurity risk management program and make updates, as necessary.
Configuration Management (Protect)	**Recommendation 4:** Develop, document, and implement a formal process to consistently capture and share lessons learned on the effectiveness of its configuration baseline program and make updates, as necessary.
	Recommendation 5: Develop, document, and implement a formal process that clearly defines [redacted] requirements for all configuration change types at the U.S. Securities and Exchange Commission or configuration changes [redacted].
Information Security Continuous Monitoring (Detect)	**Recommendation 7:** Develop, document, and implement a formal process to consistently capture and share lessons learned to improve the effectiveness of its information security continuous monitoring policies and strategy and make updates, as necessary.
Contingency Planning (Recover)	**Recommendation 8:** Develop, document, and implement a process to consistently utilize automated testing for information system contingency plan efforts, [redacted]

Source: Kearney-generated based on OIG analysis of open and closed recommendations from SEC OIG Reports No. 546, No. 552, No. 563, and No. 570

Appendix III: Summary of Assessed FISMA Ratings, FYs 2021 and 2022

TABLE 5 lists the individual *FY 2022 IG FISMA Reporting Metrics* core metric ratings for the SEC in FYs 2021 and 2022, as well as the determination of "effective" or "not effective" for each metric in FY 2022. Individual metrics are colored to highlight where the SEC improved or regressed between FYs 2021 and 2022. See the key below.

TABLE 5. Summary of Assessed FISMA Ratings between FYs 2021 and 2022

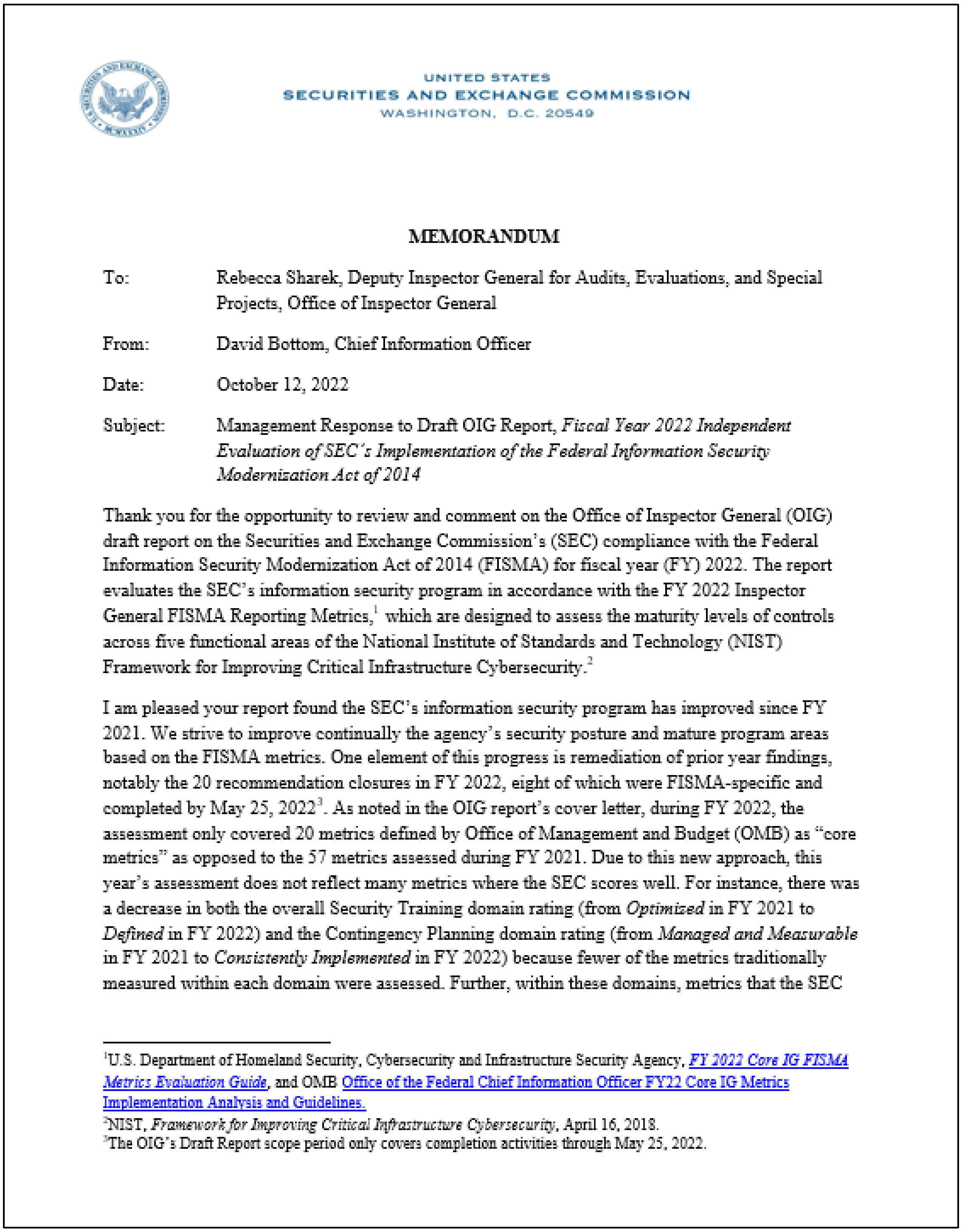
	Domain	#	Metric Title	2022 Effective/ Not Effective	Assessed Rating 2022	Assessed Rating 2021
Identify	Risk Management	1	Inventory of Information Systems and System Interconnections	Not Effective	*Defined*	*Defined*
		2	Inventory of Hardware Assets	Not Effective	*Defined*	*Consistently Implemented*
		3	Inventory of Software Assets	Not Effective	*Defined*	*Defined*
		5	Information System Security Risk	Not Effective	*Consistently Implemented*	*Consistently Implemented*
		10	Enterprise-Wide View of Cybersecurity Risks	Effective	*Optimized*	*Managed and Measurable*
	Overall		**Assessed Conclusion**	**Not Effective**	***Consistently Implemented***	***Consistently Implemented***
	SCRM	14	Acquisition and Assessment Processes for Third-Party Providers	Not Effective	*Ad Hoc*	*Ad Hoc*
	Overall		**Assessed Conclusion**	**Not Effective**	***Ad Hoc***	***Ad Hoc***
Protect	Configuration Management	20	Configuration Settings and Common Secure Configurations	Not Effective	*Defined*	*Defined*
		21	Flaw Remediation	Not Effective	*Defined*	*Defined*
	Overall		**Assessed Conclusion**	**Not Effective**	***Defined***	***Defined***
	Identity and Access Management	30	Strong Authentication- Non-Privileged	Not Effective	*Defined*	*Defined*
		31	Strong Authentication - Privileged	Not Effective	*Defined*	*Defined*
		32	Privileged Account Management	Not Effective	*Defined*	*Defined*
	Overall		**Assessed Conclusion**	**Not Effective**	***Defined***	***Defined***
	Data Protection and Privacy	36	Protection of PII and Sensitive Data	Not Effective	*Defined*	*Defined*
		37	Data Exfiltration Prevention	Not Effective	*Consistently Implemented*	*Consistently Implemented*
	Overall		**Assessed Conclusion**	**Not Effective**	***Consistently Implemented***	***Consistently Implemented***
	Security Training	42	Assessment of Cybersecurity Workforce	Not Effective	*Defined*	*Defined*
	Overall		**Assessed Conclusion**	**Not Effective**	***Defined***	***Optimized***

	Domain	#	Metric Title	2022 Effective/ Not Effective	Assessed Rating 2022	Assessed Rating 2021
Detect	ISCM	47	ISCM Policies and Strategy	Not Effective	*Consistently Implemented*	*Consistently Implemented*
		49	Ongoing Assessments	Not Effective	*Consistently Implemented*	*Consistently Implemented*
	Overall		**Assessed Conclusion**	**Not Effective**	***Consistently Implemented***	***Consistently Implemented***
Respond	Incident Response	54	Incident Detection and Analysis	Effective	*Managed and Measureable*	*Managed and Measurable*
		55	Incident Response Handling Processes	Effective	*Consistently Implemented*	*Optimized*
	Overall		**Assessed Conclusion**	**Effective**	***Managed and Measureable***	***Managed and Measureable***
Recover	Contingency Planning	61	BIA (Prev. 62)	Effective	*Defined*	*Managed and Measurable*
		63	System Contingency Planning Testing / Exercises (Prev. 64)	Not Effective	*Consistently Implemented*	*Consistently Implemented*
	Overall		**Assessed Conclusion**	**Not Effective**	***Consistently Implemented***	***Managed and Measureable***

Key:
Green: Indicates the assessed rating improved from FY 2021 to FY 2022
Red: Indicates the assessed rating regressed from FY 2021 to FY 2022

Source: Kearney-generated based on FY 2021 and FY 2022 SEC CyberScope results

Appendix IV: Management Comments



UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

MEMORANDUM

To: Rebecca Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects, Office of Inspector General

From: David Bottom, Chief Information Officer

Date: October 12, 2022

Subject: Management Response to Draft OIG Report, *Fiscal Year 2022 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014*

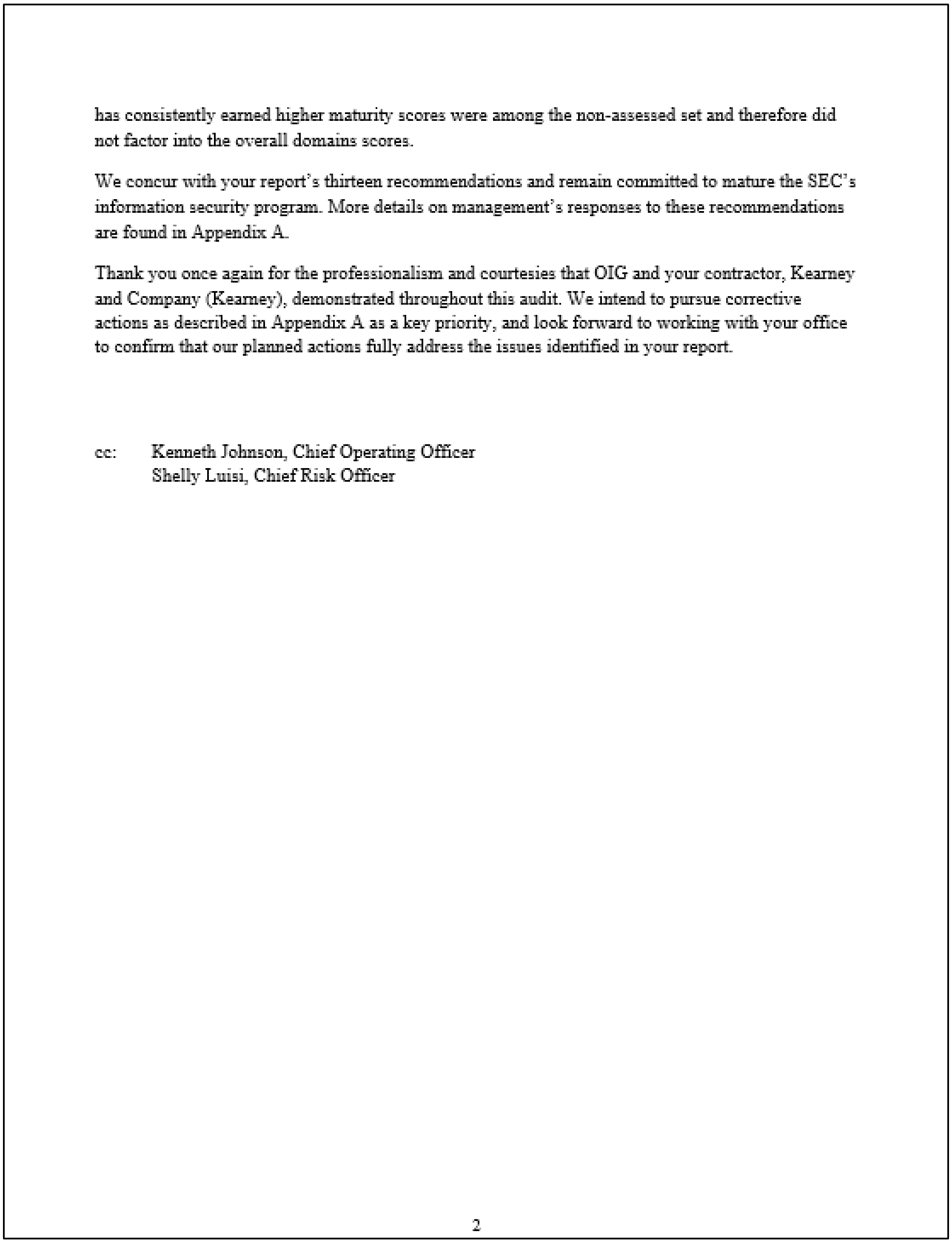
Thank you for the opportunity to review and comment on the Office of Inspector General (OIG) draft report on the Securities and Exchange Commission's (SEC) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year (FY) 2022. The report evaluates the SEC's information security program in accordance with the FY 2022 Inspector General FISMA Reporting Metrics,[1] which are designed to assess the maturity levels of controls across five functional areas of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.[2]

I am pleased your report found the SEC's information security program has improved since FY 2021. We strive to improve continually the agency's security posture and mature program areas based on the FISMA metrics. One element of this progress is remediation of prior year findings, notably the 20 recommendation closures in FY 2022, eight of which were FISMA-specific and completed by May 25, 2022[3]. As noted in the OIG report's cover letter, during FY 2022, the assessment only covered 20 metrics defined by Office of Management and Budget (OMB) as "core metrics" as opposed to the 57 metrics assessed during FY 2021. Due to this new approach, this year's assessment does not reflect many metrics where the SEC scores well. For instance, there was a decrease in both the overall Security Training domain rating (from *Optimized* in FY 2021 to *Defined* in FY 2022) and the Contingency Planning domain rating (from *Managed and Measurable* in FY 2021 to *Consistently Implemented* in FY 2022) because fewer of the metrics traditionally measured within each domain were assessed. Further, within these domains, metrics that the SEC

[1] U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *FY 2022 Core IG FISMA Metrics Evaluation Guide*, and OMB Office of the Federal Chief Information Officer FY22 Core IG Metrics Implementation Analysis and Guidelines.

[2] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, April 16, 2018.

[3] The OIG's Draft Report scope period only covers completion activities through May 25, 2022.

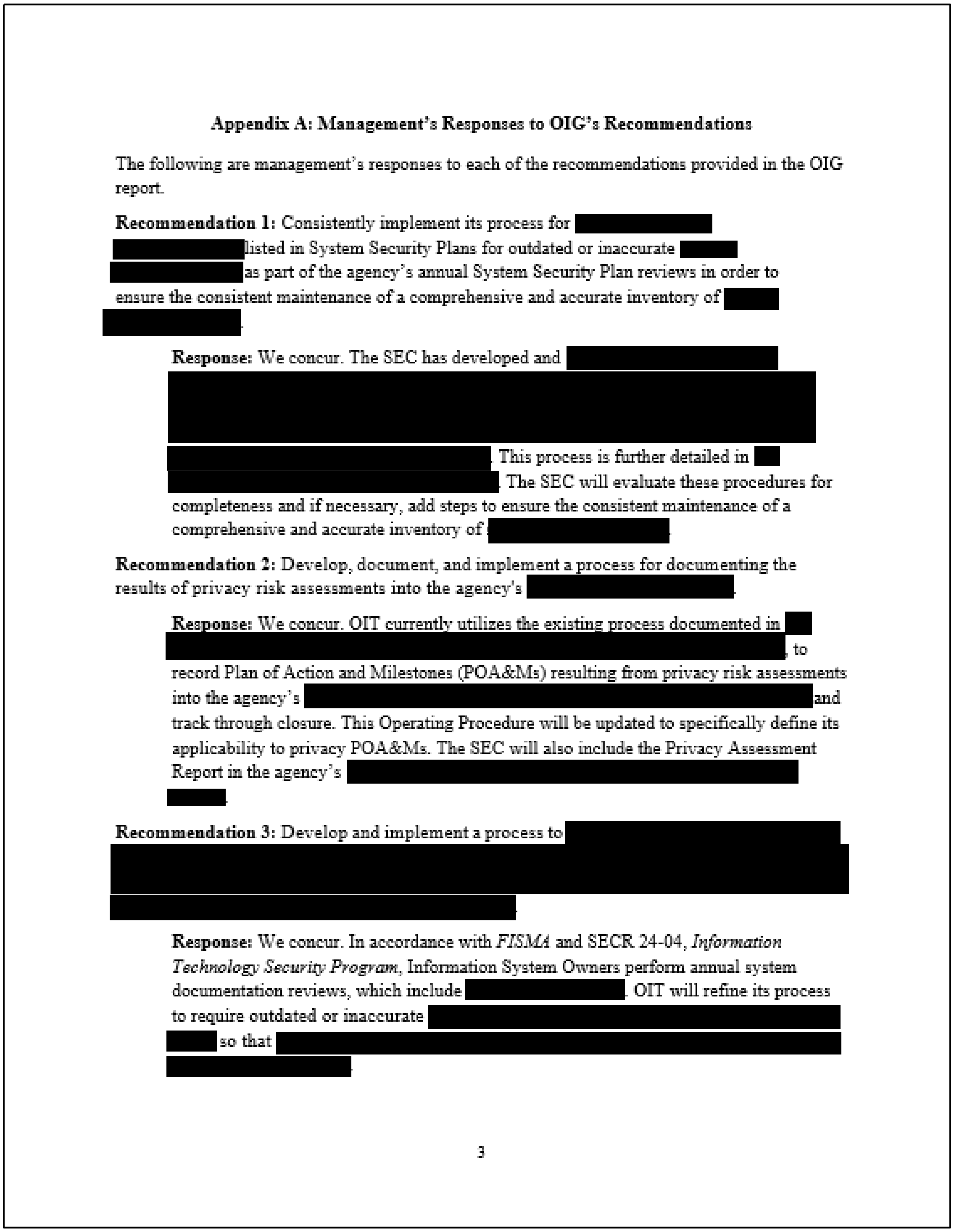


has consistently earned higher maturity scores were among the non-assessed set and therefore did not factor into the overall domains scores.

We concur with your report's thirteen recommendations and remain committed to mature the SEC's information security program. More details on management's responses to these recommendations are found in Appendix A.

Thank you once again for the professionalism and courtesies that OIG and your contractor, Kearney and Company (Kearney), demonstrated throughout this audit. We intend to pursue corrective actions as described in Appendix A as a key priority, and look forward to working with your office to confirm that our planned actions fully address the issues identified in your report.

cc: Kenneth Johnson, Chief Operating Officer
Shelly Luisi, Chief Risk Officer



Appendix A: Management's Responses to OIG's Recommendations

The following are management's responses to each of the recommendations provided in the OIG report.

Recommendation 1: Consistently implement its process for [redacted] listed in System Security Plans for outdated or inaccurate [redacted] as part of the agency's annual System Security Plan reviews in order to ensure the consistent maintenance of a comprehensive and accurate inventory of [redacted].

> **Response:** We concur. The SEC has developed and [redacted]. This process is further detailed in [redacted]. The SEC will evaluate these procedures for completeness and if necessary, add steps to ensure the consistent maintenance of a comprehensive and accurate inventory of [redacted].

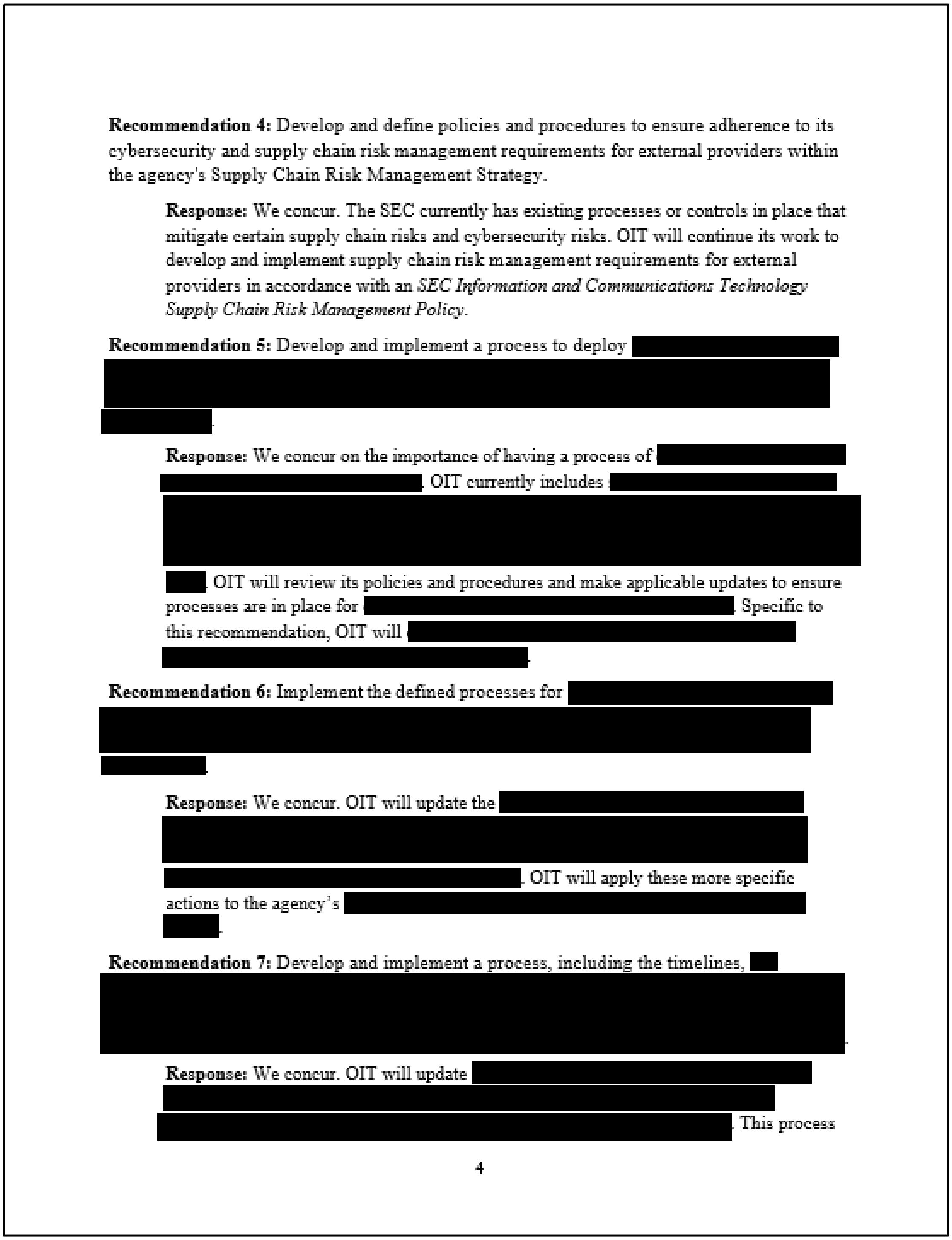
Recommendation 2: Develop, document, and implement a process for documenting the results of privacy risk assessments into the agency's [redacted].

> **Response:** We concur. OIT currently utilizes the existing process documented in [redacted], to record Plan of Action and Milestones (POA&Ms) resulting from privacy risk assessments into the agency's [redacted] and track through closure. This Operating Procedure will be updated to specifically define its applicability to privacy POA&Ms. The SEC will also include the Privacy Assessment Report in the agency's [redacted].

Recommendation 3: Develop and implement a process to [redacted].

> **Response:** We concur. In accordance with *FISMA* and SECR 24-04, *Information Technology Security Program*, Information System Owners perform annual system documentation reviews, which include [redacted]. OIT will refine its process to require outdated or inaccurate [redacted] so that [redacted].

3



Recommendation 4: Develop and define policies and procedures to ensure adherence to its cybersecurity and supply chain risk management requirements for external providers within the agency's Supply Chain Risk Management Strategy.

> **Response:** We concur. The SEC currently has existing processes or controls in place that mitigate certain supply chain risks and cybersecurity risks. OIT will continue its work to develop and implement supply chain risk management requirements for external providers in accordance with an *SEC Information and Communications Technology Supply Chain Risk Management Policy*.

Recommendation 5: Develop and implement a process to deploy [redacted].

> **Response:** We concur on the importance of having a process of [redacted]. OIT currently includes [redacted]. OIT will review its policies and procedures and make applicable updates to ensure processes are in place for [redacted]. Specific to this recommendation, OIT will [redacted].

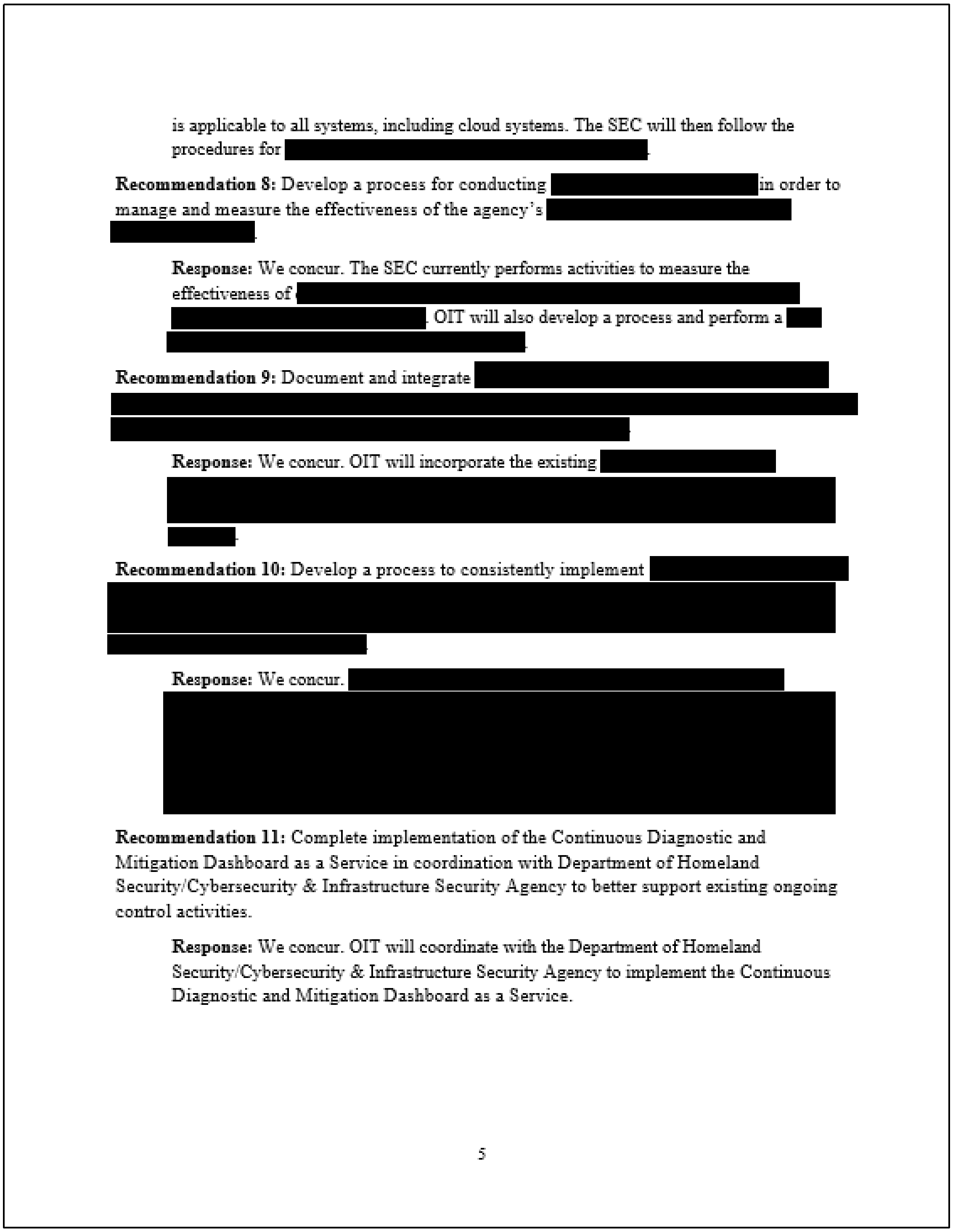
Recommendation 6: Implement the defined processes for [redacted].

> **Response:** We concur. OIT will update the [redacted]. OIT will apply these more specific actions to the agency's [redacted].

Recommendation 7: Develop and implement a process, including the timelines, [redacted].

> **Response:** We concur. OIT will update [redacted]. This process

4



is applicable to all systems, including cloud systems. The SEC will then follow the procedures for [redacted].

Recommendation 8: Develop a process for conducting [redacted] in order to manage and measure the effectiveness of the agency's [redacted].

Response: We concur. The SEC currently performs activities to measure the effectiveness of [redacted]. OIT will also develop a process and perform a [redacted].

Recommendation 9: Document and integrate [redacted].

Response: We concur. OIT will incorporate the existing [redacted].

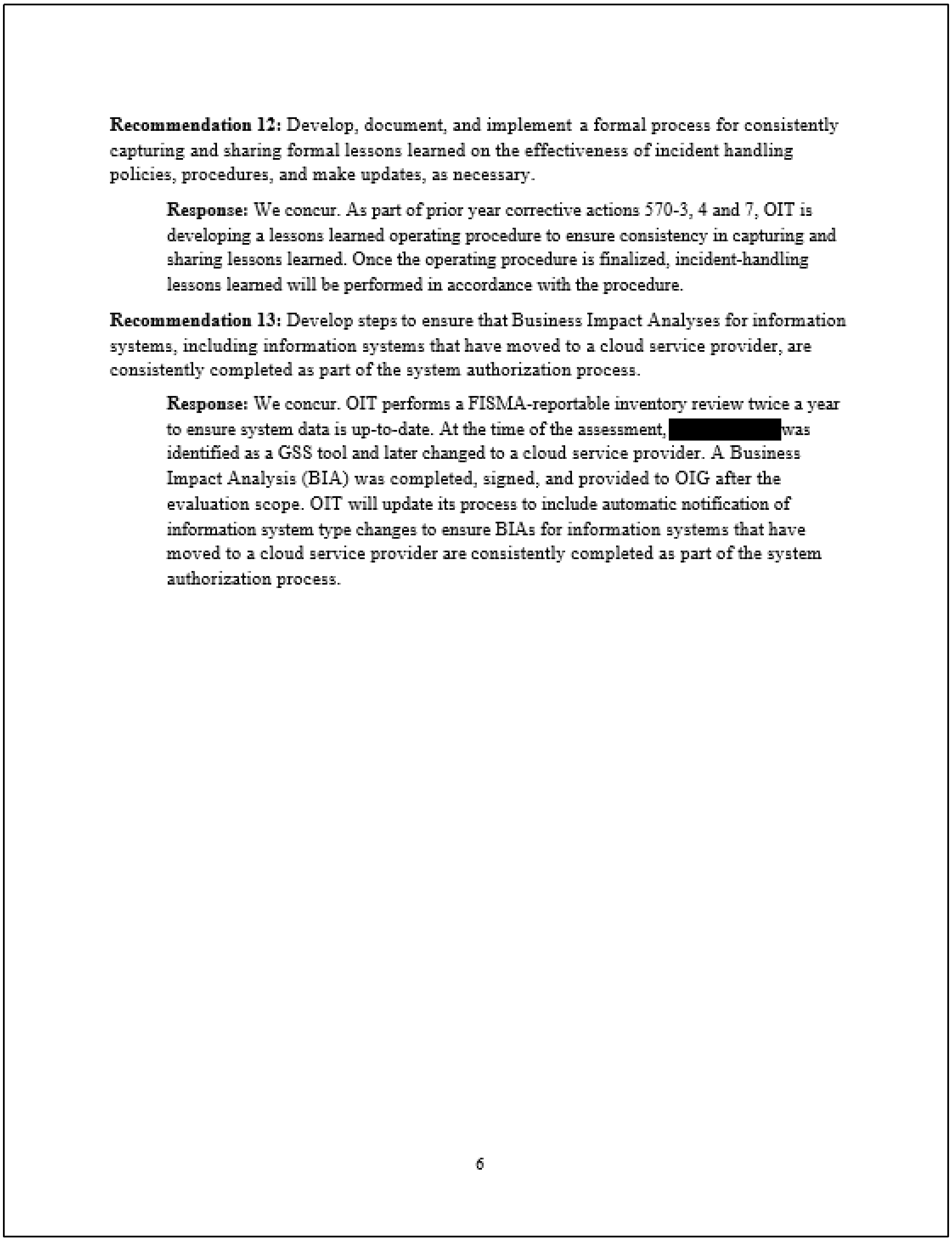
Recommendation 10: Develop a process to consistently implement [redacted].

Response: We concur. [redacted]

Recommendation 11: Complete implementation of the Continuous Diagnostic and Mitigation Dashboard as a Service in coordination with Department of Homeland Security/Cybersecurity & Infrastructure Security Agency to better support existing ongoing control activities.

Response: We concur. OIT will coordinate with the Department of Homeland Security/Cybersecurity & Infrastructure Security Agency to implement the Continuous Diagnostic and Mitigation Dashboard as a Service.

5



Recommendation 12: Develop, document, and implement a formal process for consistently capturing and sharing formal lessons learned on the effectiveness of incident handling policies, procedures, and make updates, as necessary.

> **Response:** We concur. As part of prior year corrective actions 570-3, 4 and 7, OIT is developing a lessons learned operating procedure to ensure consistency in capturing and sharing lessons learned. Once the operating procedure is finalized, incident-handling lessons learned will be performed in accordance with the procedure.

Recommendation 13: Develop steps to ensure that Business Impact Analyses for information systems, including information systems that have moved to a cloud service provider, are consistently completed as part of the system authorization process.

> **Response:** We concur. OIT performs a FISMA-reportable inventory review twice a year to ensure system data is up-to-date. At the time of the assessment, [redacted] was identified as a GSS tool and later changed to a cloud service provider. A Business Impact Analysis (BIA) was completed, signed, and provided to OIG after the evaluation scope. OIT will update its process to include automatic notification of information system type changes to ensure BIAs for information systems that have moved to a cloud service provider are consistently completed as part of the system authorization process.

Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits, evaluations, or reviews, please send an e-mail to OIG Audit Planning at AUDplanning@sec.gov. Comments and requests can also be mailed to the attention of the Deputy Inspector General for Audits, Evaluations, and Special Projects at the address listed below.

TO REPORT

fraud, waste, and abuse

Involving SEC programs, operations, employees, or contractors

FILE A COMPLAINT ONLINE AT

www.sec.gov/oig

CALL THE 24/7 TOLL-FREE OIG HOTLINE

833-SEC-OIG1

CONTACT US BY MAIL AT

U.S. Securities and Exchange Commission
Office of Inspector General
100 F Street, N.E.
Washington, D.C. 20549